

Abstract

The aim of the invention is to propose the generation, verification and denial of an undeniable signature which has a size smaller than the currently available undeniable signatures, i.e. less than 80 bits.

This aim is achieved by the method to generate an undeniable signature (y_1, \dots, y_t) on a set of data, this method comprising the following steps:

- transforming the set of data (m) to a sequence of a predetermined number (t) of blocks (x_1, \dots, x_t) , these blocks being members of an Abelian group, this transformation being a one way function,
- applying to each block (x_i) a group homomorphism (f) to obtain a resulting value (y_i) , in which the number of elements of the initial group (G) is larger than the number of elements (d) of the destination group (H) .